REMARKS

The present response is intended to be fully responsive to all points of objection and/or rejection raised by the Examiner and is believed to place the application in condition for allowance. Favorable reconsideration and allowance of the application is respectfully requested.

Applicants assert that the present invention is new, non-obvious and useful. Prompt consideration and allowance of the claims is respectfully requested.

Status of Claims

Claims **1-37** are pending in the application.

Claims **1-37** have been rejected.

Claims **1, 21**, **24** and **34** have been amended in this submission. Applicants respectfully assert that the amendments to the claims add no new matter.

Comments on Amendments After Final Rejection

Applicants are aware that the application is under final rejection, and that amendments to finally rejected claims are discouraged and not considered as a matter of right. Nevertheless, Applicants respectfully request entry of the amendments to claims 1, 21, 24 and 34. The amendments merely serve to clarify the scope of the present claims. It is respectfully submitted that entry and consideration of the requested amendments would serve to present the rejected claims in better form for consideration on appeal. Accordingly, the amendments may be admitted under 37 CFR § 1.116(b)(2).

CLAIM REJECTIONS

35 U.S.C. § 103 Rejections

In the final Office action, the Examiner rejected claims 1-20, 35 and 37 under 35 U.S.C. § 103(a), as being unpatentable over Steinberg (US Patent No. 6,587,949) in view of Mambakkam (US Publication No. 2002/0073340) and in further view of Hann et al (US Patent No. 4,799,153). Applicants traverse the rejection for at least the reasons that follow.

The Steinberg reference discloses a secure storage device for securing digital data at an acquisition stage. Generally, the Steinberg reference discloses an intermediary storage device to receive digital data from a device such as a digital camera, perform one or more security functions such as encryption of received digital data and write of the encrypted (or otherwise secured) data to a computer. In order to decrypt the encrypted data, a user operating the computer is required to use a password key.

Preliminarily, a distinction between the Steinberg reference and the claims of the present application is that the Steinberg reference is directed to securing content but is not directed to securing a transfer of the content.

Steinberg does not teach or even remotely suggest analyzing transferred data or reaching a decision whether or not to allow the transfer of the data. Rather, to the contrary, as taught by Steinberg, the secure storage device is to transfer data as an unsecured storage device or on a raw transfer level:

> The computer is able to read data on the raw transfer level as if the device is a standard unsecured storage device. (Steinberg, Abstract, emphasis added).

As disclosed by Steinberg, once encrypted (or otherwise secured) on the storage device, data is simply and unconditionally written from the storage device to the computer:

> This data is received by the storage device and secured (block 60), a process requiring a pre programmed key. The storage device then writes the secured data (block 62),

> again without requiring the receipt of a password, which is read by the computer (block 64). (Steinberg, col. 5, lines 13-16, emphasis added)

In fact, rather than analyzing data or determining whether to allow a transfer of data, Steinberg is specifically directed to simplifying the transfer of data to a computer:

> A point of novelty illustrated in FIG. 2 is that no password or key is required either to download data from the camera to the device, or from the device to a computer, as indicated in blocks 58, 62 and 64. This method allows maximum security of data, while allowing use of a standard digital camera and computer for all phases except the final step (block 65), wherein the user must load appropriate software with a key into the computer for decryption of the encrypted data. (Steinberg, col. 5, lines 57-65, emphasis added).

In contrast, independent claim 1 recites a "method for protecting the transfer of data between a computer and an external device," and further recites the elements of "analyzing, by said module, the data portion according to a protocol associated with the physical communication port", "determining, by the module, based at least in part on said data portion analysis, whether a decision on whether to allow the data communication session may be reached", "determining, by the module, based at least in part on said data portion analysis, whether to allow the data communication session" and "[if] said data communication session is not to be allowed, then modifying data transportation related to said data communication session".

None of the above elements are disclosed or even remotely suggested by Steinberg. In fact, as discussed above, these elements would serve no purpose, and indeed would be undesirable in the context of Steinberg's disclosure, which is directed to simplifying the transfer of data by allowing the use of a standard digital camera and computer for all phases, including the transfer of data from the external device to the computer, except a final step, where the user is to use a key for decryption of encrypted data.

In rejecting claim 1, to find the element of "analyzing, by said module, the data portion according to a protocol associated with the physical communication port" where

this element is comprised in a "method for protecting the transfer of data between a computer and an external device," the Examiner pointed to Steinberg col. 4, lines 4-11, which recite:

> The device 10 is configured so that the PC 16 recognizes the device 10 as a regular storage device with readable files on the file system level without the need for presenting a password. The secure data is then transferred from the device 10 to the computer 16. In order for a user to view encrypted data, the computer 16 must be programmed to decrypt the data, generally in response to entry of a password.

First, neither in the above portion, nor elsewhere, does Steinberg disclose a method for protecting the transfer of data between a computer and an external device; rather, and as discussed, Steinberg is directed to securing the data by applying various measures at the receiving storage device, e.g., encrypting the data. Regarding the transfer of the data, Steinberg does not disclose any methods or means other than writing of the data to the computer, which is the trivial solution.

Second, Steinberg does not disclose analyzing a data portion according to a protocol associated with the physical communication port. Although disclosing performing one or more security functions, such as encryption, creation of an authentication file and adding secure annotations, Steinberg does not disclose analyzing the data. In fact, as directed to securing data, analysis of the data would serve no purpose to Steinberg.

Clearly, the above portion of the Steinberg reference merely discloses a computer (PC 16) to recognize a device (device 10) as a regular storage device with readable files, transferring encrypted data from the device to the computer and using a password to decrypt encrypted data on the computer.

Accordingly, Steinberg does not disclose or even remotely suggest a "method for protecting the transfer of data between a computer and an external device," nor does Steinberg disclose or even remotely suggest the element of "analyzing, by said module, the data portion according to a protocol associated with the physical communication port" as recited in claim 1.

Furthermore, in the final Office action, the Examiner concedes that Steinberg does not disclose "determining, by the module, based at least in part on said data portion analysis, whether a decision on whether to allow the data communication session may be reached," and "determining, by the module, based at least in part on said data portion analysis, whether to allow the data communication session, wherein if said data communication session is to be allowed, then transferring the one or more data portions with data stored in the associated buffer, if any exist, toward or from the physical communication port".

To find these elements, the Examiner points to Fig. 8 and the Abstract of Mambakkam. However, as discussed below, the Mambakkam reference does not teach the claimed elements.

First, it must be noted that Mambakkam cannot cure the deficiencies of Steinberg highlighted in the above discussion.

Next, with reference to the cited claim element, Mambakkam is directed to a secured mass storage device which protects data at an access level, namely, based on an authorization procedure, a user is either authorized to access data or, if authorization fails, the access is blocked. The Abstract of Mambakkam discloses:

> An external mass storage device is secured against unauthorized access. A fingerprint reader is integrated on the external mass storage device. An initialization routine is executed when the device is plugged into a personal computer (PC) using a USB, IEEE 1394, PCMCIA, or other interface. The initialization routine scans the user's fingerprint and extracts biometric information. The biometric information is compared to stored biometric records to determine if the user is authorized to access the external mass storage device. When authorization fails, the initialization routine halts, preventing the PC from mounting the external mass storage, thus blocking access. When authentication passes, initialization continues and the external mass storage is mounted and accessible from the PC. Since the initialization routine and stored biometric records are stored on the external mass storage, the external mass storage is protected even when moved to a different PC. Special biometric security software does not have to be installed on the PC.

Mambakkam discloses a mass storage device secured against unauthorized access. However, rather than based on analyzing a portion of data being transferred during a session, in fact, before any portion of data is transferred, a determination of whether to allow the data communication session is made based on comparing extracted biometric information to stored biometric records.

Regarding Fig. 8 of Mambakkam (reproduced below), the process depicted comprises capturing a thumbprint of a user, comparing the thumbprint to a template and, if a match is found, allowing access, or, if no match is found, blocking the access. Accordingly, similarly to the Abstract, Fig. 8 does not disclose analysis of a data portion nor determining, based on such analysis, whether a decision on whether to allow the data communication session can be reached. Likewise, Fig. 8 does not disclose determining, based on such analysis, whether to allow the data communication session, nor does Fig. 8 disclose if said data communication session is to be allowed, then transferring the one or more data portions with data stored in an associated buffer, if any exist, toward or from the physical communication port.

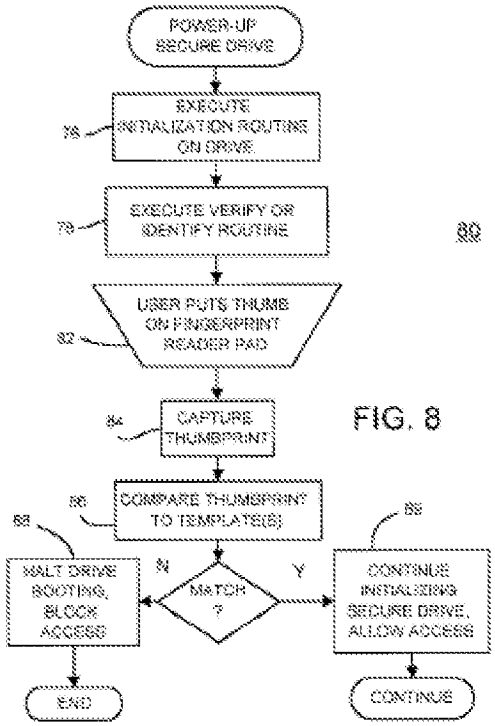

FIG. 8

Accordingly, Mambakkam discloses determining if a user is authorized to access an external mass storage device prior to any portion of data is being transferred, and, consequently, does not disclose or even remotely suggest "determining, by the module, based at least in part on said data portion analysis, whether a decision on whether to allow the data communication session may be reached," and "determining, by the module, based at least in part on said data portion analysis, whether to allow the data communication session, wherein if said data communication session is to be allowed, then transferring the one or more data portions with data stored in the associated buffer, if any exist, toward or from the physical communication port" as recited by claim 1.

In the final Office action, the Examiner further concedes that the combination of the Steinberg and Mambakkam references does not disclose "[and] if said data communication session is not to be allowed, then modifying data transportation related to said data communication session."

The Examiner further concedes in the final Office action that the combination of the Steinberg and Mambakkam references does not disclose "[wherein] if no decision may be reached on whether to allow, then storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' and waiting for a next data portion, and if said decision may be reached, then proceeding to step 'd'".

To find these elements, the Examiner pointed to the Hann reference, at lines 11-18 in the Abstract, and col. 10, lines 63-68.

Primarily, it must be noted that the Hann reference is directed to securing a communication between a terminal and a computer, and specifically, to authenticating a user. Accordingly, the Hann reference discloses various security measures which are applied or performed prior to a communication session but is not directed to securing a transfer of data between a computer and an external device. As disclosed by Hann, a security device generates an initial data packet indicative of a user authorization. A host security device intercepts and processes the initial data packet and, if user authorization is indicated therein, enables establishment of a communication session.

Applicants note that the initial data packet disclosed by Hann is not part of the communication session. Rather, the initial data packet is generated, communicated and processed as part of an authentication process performed prior to the data communication session. In fact, as disclosed by Hann, the initial data packet is unsuited for processing by the addressed processor:

> Security of communications in a packet-switched data communications system is enhanced by introducing terminal and host security devices into the system in communicative relationship with a terminal and a host processor, respectively. In response to a user-initiated data entry at the terminal, the terminal security device generates an initial data packet indicative of user authorization or not, but which is unsuited for processing by the addressed processor, ahead of additional data packets containing user-entered message data to be processed by the addressed processor. (Hann, Abstract, emphasis added)

Accordingly, the initial data packet disclosed by Hann can not be considered "a data portion during a data communication session" simply because when the initial data packet is generated, communicated and processed, the communication session has not yet been established, rather, the communication session is to be established or prevented based on the processing of the initial data packet. The Abstract of the Hann reference, at lines 11-18 discloses:

> The host security device intercepts and processes the initial data packet and, if user authorization is indicated therein, replaces it with an artificial data packet solely to render the additional packets amenable to processing by the addressed processor and thereby to establish a communications session between user terminal and processor-associated database to which access was requested. (emphasis added).

Clearly, rather than disclosing "storing the data portion in a buffer, wherein the buffer is associated with the data communication session" lines 11-18 in the Abstract of Hann disclose the initial data packet is replaced with an artificial data packet. Furthermore, col. 10, lines 63-68 discloses:

> Data control information is stored in buffer storage 20, which has a capacity of eight kilobytes. The IBM-PC system board accesses buffer storage 320 via I/O channel

> 310. LAPB controllers 306 and 308 also access data and control information contained in buffer storage 320.

The above portion of Hann merely discloses storing data control information in a buffer and means known in the art (e.g., an I/O channel) for accessing buffers. In addition, Applicants note that the architecture disclosed in the Hann reference is related to the host security device which, as disclosed by Hann, intercepts, processes and replaces the initial data packet but does not capture, intercept or otherwise obtains data packets related to the data communication session. Rather, once a user is authenticated, data flows directly between the addressed processor and the authorized user terminal.

Accordingly, storing a data portion associated with the data communication session would serve no purpose to Hann, consequently, Hann does not disclose or render such element obvious.

Furthermore, as disclosed by Hann, a single artificial data packet is generated, communicated, processed and replaced. Accordingly, the element of "storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' and waiting for a next data portion" would likewise serve no purpose to Hann.

Therefore, the Hann reference, like the Steinberg and Mambakkam references, does not disclose neither "[and] if said data communication session is not to be allowed, then modifying data transportation related to said data communication session." nor "[wherein] if no decision may be reached on whether to allow, then storing the data portion in a buffer, wherein the buffer is associated with the data communication session and returning to step 'a' and waiting for a next data portion, and if said decision may be reached, then proceeding to step 'd'". as recited by claim 1.

Accordingly, claim 1, and claims 2-20, 35 and 37 dependent therefrom, are allowable over any combination of the Steinberg, Mambakkam and Hann references.

Some of the dependent claims merit further discussion. Regarding claim 2, neither Steinberg nor Mambakkam or Hann teach "wherein the step of modifying the data transportation comprises blocking the transportation." As discussed, since the cited

references do not teach nor are they directed to modifying (or otherwise manipulating) the actual data, they consequently do not block a session based on the data communicated over the session.

Likewise, regarding claims 3-5, Applicants respectfully assert that since the cited references do not teach nor are they directed to modifying (or otherwise manipulating) the actual data, none they do not disclose "wherein the step of modifying the data transportation comprises modifying a status of a requested file," as recited.

Regarding claims 6-8, 11, 15 and 18, the Hann reference is directed to a computer connected to a network, the Mambakkam reference is directed to a computer connected to a mass storage device and the Steinberg reference is directed to a computer connected to a standard unsecured storage device. Accordingly, none of the cited references are directed to nor teach a specific physical communication port.

Regarding claims 9-10, as discussed, the Steinberg reference teaches encrypting data and then writing the data to a computer, the Mambakkam reference teaches allowing or blocking access to a mass storage device and the Hann reference teaches authenticating a user prior to permitting access over a network, however, none of the cited references teaches analyzing data being communicated during a session, neither according to a higher level protocol nor otherwise.

Regarding claims 12-14 and 37, none of the references teach buffering data, neither in order to analyze the data nor for any other purpose. In fact, none of the references stand to gain any advantage by buffering data. For example, as taught by Steinberg, once decrypted, data (e.g., images from a camera) is simply written to the computer. As taught by Mambakkam, once a user is authenticated, access to the mass storage device is enabled and no buffering is required. Likewise, according to Hann, once a user is authenticated, there is no reason or motivation to buffer data related to the session.

Accordingly and for these reasons too, claims 2-20, 35 and 37, are allowable over the the Steinberg, Mambakam and Hann references.

In the Office action, the Examiner rejected claims 1-15 and 17-35 under 35 U.S.C. § 103(a), as being unpatentable over Nickles (US Patent No. 6,134,591) in view of Hann. Applicants traverse the rejection for at least the reasons that follow.

Similarly to the Hann reference discussed above, the Nickles reference is directed to authenticating a user prior to allowing data to be transferred. Furthermore, Nickles is neither directed to, nor teaches, a transfer of data between a computer and an external device connected to the computer but rather, to authenticating a user prior to allowing a transfer of data over a network.

Accordingly, since, as taught by Nickles, authentication of a user is performed prior to allowing or enabling any data transfer between the user and the destination computer, at least "receiving, by a module on the computer, a data portion during a data communication session between the computer and the external device" as recited by independent claim 1 is not taught by neither the Nickles nor Hann references.

In fact, as taught by Nickles, once a user is authenticated, data is allowed to flow freely over the network between the user and the destination computer. Accordingly, receiving a data portion during a data communication session would serve no purpose to Nickles and, consequently, would not be obvious to a person having ordinary skill in the art.

Accordingly, the discussion above regarding the rejection of claims 1-20, 35 and 37 in view of Hann is relevant to Nickles.

Applicants have amended independent claim 21 to recite a "system for protecting the transfer of data between a computer coupled to a private network and an external device" to further clarify the scope of the invention which is directed to a transfer of data between an external device and a computer, unlike the Nickles reference.

Applicants have further amended independent claims 21 and 34 to recite elements similar to those recited by independent claim 1 and discussed above at length.

Applicants have amended independent claim 24 to recite a "security policy includes a plurality of rules related to at least a content of the data portion and a type of an operation that can be performed during the communication session." to further clarify the scope of the invention which is directed to enabling or preventing a transfer of data between an external device and a computer, unlike the Nickles reference.

Accordingly, Applicants submit that independent claims 1, 21 and 34 are allowable over the combination of Hann and Nickles. Claims 2-15, 17-20, 22-33, and 35 which depend from allowable independent claims are likewise allowable over the the combination of Hann and Nickles.

In view of the foregoing amendments and remarks, Applicants assert that the pending claims are allowable. Their favorable reconsideration and allowance is respectfully requested.

Should the Examiner have any question or comment as to the form, content or entry of this Amendment, the Examiner is requested to contact the undersigned at the telephone number below. Similarly, if there are any further issues yet to be resolved to advance the prosecution of this application to issue, the Examiner is requested to telephone the undersigned counsel.

Please charge any fees associated with this paper to deposit account No. 50-3355.

Respectfully submitted,

/Guy Yonay/
Guy Yonay
Attorney/Agent for Applicants
Registration No. 52,388

Dated: August 20, 2010

Pearl Cohen Zedek Latzer, LLP
1500 Broadway, 12th Floor
New York, New York 10036
Tel: (646) 878-0800
Fax: (646) 878-0801